# Microsoft trop lent à corriger quatre failles zero-day dans Internet Explorer | Le Net Expert Informatique

## Microsoft trop lent à corriger quatre failles zero-day dans Internet Explorer

**Alerté en janvier par TippingPoint (HP) de l'existence de 4 vulnérabilités d'Internet Explorer, Microsoft avait plus de 6 mois pour les corriger. Le délai écoulé et faute de correctifs, des détails sur ces vulnérabilités ont été divulgués.**

Microsoft se montre une nouvelle fois trop lent à corriger des vulnérabilités dans ses logiciels. C'est Internet Explorer, son navigateur, qui est à présent pointé du doigt par la Zero Day Initiative de TippingPoint, une filiale d'HP.
Les spécialistes des failles logicielles accordent six mois aux éditeurs pour corriger des vulnérabilités signalées avant de dévoiler publiquement leur existence. Et c'est ce qui vient de se produire pour quatre failles d'Internet Explorer.

**Interaction avec la cible requise**
Faute de correctifs une fois le délai écoulé, la ZDI a donc communiqué sur ces vulnérabilités zero-day du navigateur. Ces failles avaient été signalées en janvier 2015 à Microsoft qui n'a pas fourni de correctifs et avait demandé, et obtenu, une extension jusqu'au 19 juillet.
Les chercheurs en sécurité de TippingPoint précise que ces vulnérabilités permettent à un attaquant d'exécuter du code à distance sur les installations vulnérables d'Internet Explorer.
Pour s'exécuter, l'attaque nécessite cependant une interaction avec l'utilisateur au travers d'une visite sur une page (lien transmis dans un email ou par messagerie instantanée) ou l'ouverture d'un fichier malveillant.
Microsoft se trouve à présent confronté à l'obligation de corriger quatre failles critiques dans Internet Explorer. ZDI ne précise pas quelles sont les versions du navigateur affectées.

---



---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/zdi-microsoft-trop-lent-a-corriger-quatre-failles-zero-day-dans-internet-explorer-39822812.htm

# Augmentation de la taille moyenne d’attaques DDoS | iTPro.fr | Le Net Expert Informatique


## Augmentation de la taille moyenne d’attaques DDoS

**Arbor Networks, spécialiste de la protection contre les attaques DDoS, publie ses statistiques relatives aux attaques DDoS pour ce second trimestre.**

Tant en bits par seconde qu'en paquets par seconde, il semblerait que les attaques de type DDoS soient de plus en plus imposantes. L'attaque la plus forte de ce second trimestre de type « UDP Flood » a atteint 196 bits/s. Le problème réside surtout dans le fait que cette amplitude n'est plus aussi rare qu'auparavant.Au deuxième trimestre, 21 % d'entre elles ont dépassé 1 Gbit/s, la progression la plus forte enregistrée étant celle dans la fourchette des 2 à 10 Gbit/s. Le mois de juin a aussi été marqué par l'augmentation des attaques entre 50 et 100 Gbit/s principalement de type « SYN Flood » ciblant le Canada et les Etats-Unis.
Darren Anstee, directeur des technologies de sécurité pour Arbor Networks explique que« si les attaques d'une ampleur extrême monopolisent les gros titres, c'est la progression de la taille moyenne des attaques DDoS qui inquiète les entreprises à travers le monde. Les entreprises doivent définir clairement leur risque en matière de DDoS. Face à des attaques moyennes capables de saturer l'accès Internet de bon nombre d'entreprises, il est essentiel de saisir les risques et les coûts d'une attaque et de mettre en place les plans, services et solutions appropriés. »
Du côté des attaques par amplification et réflexion, il semblerait que celles exploitant SSDP soient en baisse puisque 84 000 ont été détectées au second trimestre contre 126 000 au deuxième. Cependant, la taille moyenne des attaques d'amplification par réflexion DNS, NTP, SSDP et Chargen a augmenté au deuxième trimestre 2015 et 50 % de ce type d'attaques ciblaient le port UDP 80 (HTTP/U) pour une durée de 20 minutes (contre 19 pour le premier). A noter que ce type d'attaque permet d'amplifier la volumétrie du trafic par un nombre de réponses envoyé plus important tout en masquant les sources. Cette technique exploite notamment le manque de mesures mises en place par les opérateurs pour filtrer le trafic et la mauvaise configuration d'équipement fournissant des services UDP.

---



---



Source : http://www.itpro.fr/n/augmentation-taille-moyenne-dattaques-ddos-21404/

# Carte de France des barrages des éleveurs en colère | Le Net Expert Informatique

| | |
|---|---|
| | Carte de France des barrages des éleveurs en colère |

Départ en vacances ? départ en congés ? Même si ça n'a aucun rapport avec la Cyber ou la Protection des données personnelles, il vous a semblé utile et même indispensable pour certains de partager avec vous la carte de France des barrages placés par des éleveurs en colère.Cette carte est intéractive et est mise à jour régulièrement par Le Figaro.
Denis JACOPINI

CENTRE-EST
Les éleveurs de Rhône-Alpes ont commencé à bloquer l'accès Nord et Est de Lyon mercredi soir avec des tracteurs, L'A6 et l'A42 étant coupées en direction de Lyon, selon Bison Futé. Ils devaient, au petit matin jeudi, paralyser l'accès Sud de la deuxième agglomération de France, selon la FNSEA régionale. À Clermont-Ferrand, la FDSEA et les JA du Puy-de-Dôme prévoyaient de bloquer cinq accès de la ville jeudi matin. Leur principale revendication: une intervention des pouvoirs publics pour faire monter les prix de la viande et du lait, élément fondamental qui ne figure pas, selon eux, dans le plan d'aide du gouvernement de 600 millions d'euros.
Mercredi, 300 à 400 agriculteurs ont bloqué cinq accès à Chalon-sur-Saône. Ils ont levé les barrages vers 22H00, selon la FDSEA de Saône-et-Loire, qui n'excluait pas de nouvelles actions jeudi matin. D'autres actions étaient prévues jeudi en Bourgogne, dans l'Yonne et la Nièvre, alors que François Hollande devait se rendre à Dijon, où il rencontrera la monde agricole à 9H00. Dans l'Yonne, ils prévoient des RASD de bloquer l'abattoir de Migennes avant de se rendre à la laiterie Yoplait de Montéteau.
Dans la région voisine de Franche-Comté, 150 à 200 agriculteurs, aux volants d'une quarantaine de tracteurs, se sont réunis mercredi soir à Vesoul (Haute-Saône), selon un correspondant de l'AFP. Les agriculteurs ont notamment «intercepté» une citerne laitière d'environ 15.000 litres de lait. Ils l'ont conduite aux abords d'une grande surface du centre-ville, où ils ont commencé à en déverser le contenu vers 23H00.

CENTRE
Mercredi soir quelque 150 agriculteurs -avec une trentaine de tracteurs- se sont mobilisés pour bloquer les livraisons à un supermarché Lidl à Savigny (au sud de Tours), selon un dirigeant de la FDSEA d'Indre-et-Loire. Du fumier, de la paille et des pneus usé été déversés pour boucher l'accès aux camions. Et les agriculteurs envisagent de cibler aussi un atelier de découpe de viande bovine à Montbazon (entre Savigny et Tours) qui, selon la FDSEA, ne traite que de la viande de provenance étrangère.

CENTRE-OUEST
Les barrages filtrants mis en place mercredi sur les routes d'accès au château de Chambord ont été levés.
«On a l'impression que Stéphane Le Foll s'en fouts de nous.»
Le président des JA du département, Charles Guerlais.
En Loire-Atlantique, où aucun blocage n'aurait lieu ce mercredi, les actions prévues jeudi matin, suivant un mot d'ordre national appelant à viser les transformateurs, sont maintenues, selon le président des JA du département, Charles Guerlais. «Les annonces du gouvernement n'ont rien fait pour calmer l'élevage (...). Dans les campagnes, on a l'impression que M. Le Foll s'en fouts de nous», a-t-il affirmé.
En Vendée, le dernier point de blocage, le péage de Beaufief, a été levé. En Charente-Maritime, le blocage perdure sur le pont de l'Ile d'Oléron. «Sauf urgences médicales», les barrages filtrants ne laissent passer qu'une cinquantaine de véhicules toutes les 45 minutes, sur une file, puis sur l'autre, selon la préfecture.
Dans la Vienne, la circulation reste fortement perturbée autour de Poitiers. L'autoroute A20, reliant Paris à Toulouse, était bloquée dans les deux sens jeudi matin en Haute-Vienne par des éleveurs en colère, qui ont mis en place un barrage filtrant, a-t-on appris auprès des agriculteurs. L'opération de blocage, menée conjointement par les éleveurs de Haute-Vienne et de Creuse, a commencé peu avant 10h00, à quelques kilomètres de la Souterraine. Toutes les voies de l'autoroute sont neutralisées au niveau du rond-point de la Croisière, qui permet l'accès à la RN 145, axe routier important pour les poids-lourds, selon le Centre régional d'information routière.

CORRÈZE
À Brive-La-Gaillarde, dans la nuit de mercredi à jeudi, quelques 200 éleveurs et agriculteurs, certains avec leur tracteur, ont déversé du lisier devant plusieurs supermarchés et fournisseurs de restaurants (Metro, Promocash), a constaté un photographe de l'AFP. Ils ont également mis le feu à des pneus et dégradé plusieurs panneaux portant les enseignes des supermarchés, selon la même source.

HAUTES-PYRÉNÉES
Plusieurs centaines d'agriculteurs de la FDSEA et des JA des Hautes-Pyrénées ont déversé mercredi soir du fumier et du lisier devant des grandes surfaces de Tarbes et son agglomération, a-t-on appris auprès des manifestants et de la préfecture. Selon un responsable agricole local, Jean-Luc Gaubet, un rassemblé peu avant minuit plusieurs centaines d'agriculteurs et près de cent tracteurs engagés dans l'action devant 12 établissements. À la préfecture on faisait état de chiffres similaires portant de 300 personnes et 125 tracteurs au total mobilisés devant 12 grandes surfaces.

NORMANDIE
Les barrages ont disparu sur le périphérique de Caen, épicentre de la contestation, après un appel des dirigeants agricoles à suspendre le mouvement quelques heures après l'annonce du plan de l'«exécutif.
Ce mot d'ordre est d'aller renforcer les barrages des ponts.» Stéphane Dauchelé, vice-président de la FNSEA de Seine-Maritime.

En Haute-Normandie, l'un des trois grands ponts suspendus permettant de traverser la Seine entre Rouen et l'estuaire, celui de Tancarville, reste bloqué, tandis que les barrages sont devenus filtrants aux ponts de Normandie et de Brotonne. «Des collègues du Calvados ont commencé leur mouvement dimanche soir, nous n'avons démarré qu'hier matin, on peut encore tenir», a déclaré à l'AFP Stéphane Dauchelé, vice-président de la FNSEA de Seine-Maritime. «Le mot d'ordre est d'aller renforcer les barrages des ponts», a ajouté M. Dauchelé.
Des éleveurs bloquent à nouveau jeudi matin les accès au Mont Saint-Michel, qu'ils avaient dégagés la veille au soir après l'annonce d'une aide d'urgence du gouvernement, a annoncé la préfecture de la Manche.Les deux routes qui donnent accès à ce site touristique, l'un des plus visités de France, la RD976 est entièrement bloquée par une dizaine de tracteurs, tandis que la RD275 reste en cours de blocage, selon la préfecture.

BRETAGNE
En Ille-et-Vilaine, la situation est revenue à la normale sauf à Saint-Malo où les éleveurs bloquent depuis mardi le principal accès à la cité corsaire. Dans le Finistère, les éleveurs qui quitté le grand pont de l'Iroise, à Brest, qu'ils occupaient depuis mardi mais celui-ci reste fermé pour sa remise en état. En revanche, d'autres barrages perduraient notamment à Quimper ou Morlaix. Dans un communiqué, les Bonnets rouges ont appelé «tous les Bretons à se joindre aux manifestations des agriculteurs partout où c'est possible».

OISE
À Lille, le blocage de l'A1 a été levé tôt dans la matinée et en Picardie, les dernières actions d'envergure ont été levées.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
Formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plaît ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lefigaro.fr/actualite-france/2015/07/22/01016-20150722ARTFIG00111-eleveurs-en-colere-la-carte-de-france-des-barrages.php

---

# Au Journal officiel, l’encadrement des mouchards de Skype (et assimilés) | Le Net Expert Informatique

| | |
|---|---|
| Après les yeux, les oreilles<br>Crédits :<br>alphaspirit/iStock/Thinkstock | Au Journal officiel, l’encadrement des mouchards de Skype (et assimilés) |

**Journal officiel, un arrêté vient encadrer, sous l'œil de l'ANSSI, la définition des mouchards que les juges peuvent désormais utiliser pour faire espionner non seulement les données saisies au clavier ou affichées sur l'écran, mais également celles « reçues et émises par des périphériques audiovisuels ».**

En 2011, la loi d'orientation et de programmation pour la sécurité intérieure (LOPPSI) avait permis à la police, sur autorisation d'un juge, la mise en place de mouchard, même à distance. L'enjeu ? Enregistrer les frappes au clavier (keylogger) ou les images affichées sur un écran afin d'espérer glaner quelques preuves, dans le cadre d'enquête pour des infractions sérieuses (criminalité organisée, terrorisme).
Seulement, il y avait un trou dans la raquette. En visant les données affichées « sur un écran » ou celles introduites « par saisie de caractères », le texte initial excluait mécaniquement la captation de parole. Une lacune très contrariante pour qui veut épier une conversation sur Skype par exemple.

**La loi contre le terrorisme et Skype**
La loi contre le terrorisme de novembre 2014 a comblé la faille. Depuis, non seulement les données saisies au clavier peuvent être espionnées judiciairement, mais également celles « reçues et émises par des périphériques audiovisuels ». La rustine se trouve à l'article 706-102-1 du Code de procédure pénale.
Toutefois encore, une dernière étape manquait pour parfaire ce système. Un autre article, le 226-3 du Code pénal, soumet ces armes de surveillance intrusive à un arrêté du Premier ministre, épaulé par le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Son objet ? Dresser la liste de ces outils sensibles dont est autorisée la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente. Sans ce feu vert, ces mêmes opérations, susceptibles de générer des atteintes à la vie privée ou au secret des correspondances, sont en effet sanctionnées de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Cet arrêté du 4 juillet 2012 « fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal » n'avait pas non plus été mis à jour depuis la loi contre le terrorisme. Cet oubli empêchait donc la commercialisation sous contrôle de mouchards de nouvelle génération.
Ce nouveau manque a été corrigé aujourd'hui au Journal officiel. Le Premier ministre a en effet complété le texte de 2012 en y remplaçant l'expression « ou telles qu'il les y introduit par saisie de caractères » par les mots « telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ». Sous l'œil de l'ANSSI, certains espiogiciels capables de surveiller Skype (et assimilés) peuvent donc maintenant être introduits en France et utilisés par les services autorisés.

**De la surveillance judiciaire à la surveillance administrative**
Rappelons au passage que le projet de loi Renseignement permet elle aussi la captation des données informatiques dans un cadre cette fois strictement administratif. Donc sans juge. La même loi s'est servie de l'article 226-3 du Code pénal pour également étendre l'aspiration des métadonnées.
Pour la poursuite de finalités jugées très floues, les services du renseignement pourront en effet utiliser l'ensemble des appareils mentionnés à cet article, afin de moissonner « les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés ». Cet arsenal (IMSI catcher, mais pas seulement) pourra par exemple être utilisé pour connaître « directement » les données générées par un smartphone, situé à proximité d'un point déterminé.

---



---



Source :
http://www.nextinpact.com/news/95893-au-journal-officiel-encadrement-mouchards-skype-et-assimiles.htm
Par Marc Rees

# Inquiétude sur les données de connexion | Le Net Expert Informatique

## Inquiétude sur les données de connexion

**C'est, pour le Conseil constitutionnel, un petit tour de chauffe avant sa décision, vendredi 24 juillet, sur la loi renseignement, un mois après avoir été saisi par le président de la République et 106 parlementaires. Le Conseil examinait en effet, mardi 21 juillet, une question prioritaire de constitutionnalité (QPC), transmise par le Conseil d'Etat, sur la délicate surveillance des données Internet.**

Trois associations (French Data Network, la Quadrature du Net et la Fédération des fournisseurs d'accès à Internet associatifs) attaquaient un article décisif, repris par la loi renseignement, de la loi de programmation militaire de décembre 2013 sur « l'accès administratif [policier] aux données de connexion » qu'elles jugent contraire « aux droits au respect de la vie privée, à un procès équitable et à la liberté de communication ».
Les associations s'inquiètent d'une mesure, introduite dans le code de la sécurité intérieure, qui autorise « le recueil, auprès des opérateurs de communications électroniques, (…) des informations et documents traités ou conservés par leurs réseaux ».

**Que sont exactement ces « informations et documents » ? Les données de connexion ? Le contenu des correspondances ?**
La loi ne le dit pas et a donc, pour les associations, délégué au pouvoir réglementaire – à l'administration – le soin de faire pour le mieux. Ça ne se fait pas. Le Conseil constitutionnel supporte mal de voir « reporter sur des autorités administratives ou juridictionnelles le soin de fixer des règles dont la détermination…
Lire la suite….

---



---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemonde.fr/societe/article/2015/07/22/inquietude-sur-les-donnees-de-connexion_4693599_3224.html
Par Franck Johannès

# Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team | Le Net Expert Informatique

| | |
|---|---|
|  | Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team |

**Anticipant sur les besoins de ses clients, Hacking Team s'est assuré d'être prêt au lancement de Windows 10. La société italienne a adapté ses outils pour être capable d'installer un backdoor sous Windows 10, et ainsi de pouvoir collecter à distance toutes les frappes de touches au clavier.**

Windows 10 n'est pas encore officiellement sorti, mais les firmes qui fournissent aux autorités les outils permettant d'accéder à distance aux données sont déjà à pied d'oeuvre pour s'adapter au niveau système d'exploitation de Microsoft. Ainsi l'entreprise italienne Hacking Team, dont les e-mails ont fuité ce mois-ci, s'est assurée dès l'an dernier de pouvoir fournir à ses clients de quoi espionner des utilisateurs de Windows 10.

« Nous avons testé Windows 10 Preview et ça fonctionne », a ainsi expliqué Marco Valleri, le directeur de Hacking Team, dans un e-mail du 4 novembre 2014. Il répondait à l'ancien responsable des opérations à Singapour, Serge Woon, qui se demandait si « RCS 9.4 supporte Windows 8.2 » (en fait Windows 10). RCS est l'acronyme de « Remote Control System », le malware qui permet à Hacking Team de prendre à distance le contrôle d'un ordinateur pour accéder à ses données.

Un autre e-mail du 29 juin 2015 montre que deux employés de Hacking Team, Marco Fontana et Andrea Di Pasquale, ont testé avec succès l'installation hors ligne de plusieurs outils sur Windows 10 Enterprise Insider Preview. Ils disent avoir vérifié notamment « l'installation d'un backdoor », « l'exportation de preuves depuis le backdoor », et la « désinstallation du backdoor ».

« Super ! », s'enthousiasme le directeur technique Marco Valleri, qui propose aussitôt une réunion pour déployer la mise à jour dans un git, probablement celui de RCS.

La société Hacking Team dispose également d'un outil invisible pour Windows 10 permettant de collecter toutes les frappes de touches au clavier (un « keylogger »), comme le montre un courriel du 5 juin. Marco Fontana, qui semble être une petite star dans l'entreprise, y rend compte d'une réunion du mercredi 3 juin 2015, où « l'un des thèmes de la réunion était le test du mécanisme d'injection dans l'application Metro ».

Il explique que « le POC du keylogger pour Windows 10 est prêt et peut être testé pour vérifier sa « compatibilité » avec les antivirus ». Le POC (Proof-of-concept) est une démonstration de faisabilité.

Dans un e-mail du 15 juin, Marco Fontana précise à son équipe qu'il a testé une « technique d'injection dans l'application Metro de Windows 10 », et que « l'exécutable 'ExeLoader' injecte la DLL ApiHookDll dans un processeur notepad.exe et capture les touches ». Il s'agit d'un POC visant à collecter les touches tapées sous sur l'application « Bloc Notes » de Windows 10.

« Si tout fonctionne correctement, dans le dossier temporaire de Windows (%temp%) vous verrez un fichier texte créé qui contient les touches enfoncées dans notepad. Le fichier a un préfixe KBD_ et une valeur aléatoire (ex: KBD_000407E600C553CE.txt) ».

Tout l'objet du logiciel RCS de Hacking Team est justement d'installer à distance les backdoors qui permettent d'installer des outils tels que ce keylogger, lequel permet ensuite de récupérer, par exemple, les mots de passe saisis pour accéder à des comptes e-mail, ou des mots de passe de clés de chiffrement.

« On ne peut pas croire à la sécurité d'un OS pour le grand public », s'était amusé en novembre dernier David Vincenzetti, le président de Hacking Team, en lisant une actualité selon laquelle Windows 10 pourrait signer la fin des malwares.

---



---



Source : http://www.numerama.com/magazine/33727-deja-des-backdoors-et-keyloggers-pour-windows-10-chez-hacking-team.html
par Guillaume Champeau

# Norauto inaugure la « révision connectée » grâce au boîtier Xee | Le Net Expert Informatique

| | |
|---|---|
| | Norauto inaugure la « révision connectée » grâce au boîtier Xee |

**Les clients Norauto pourront, bientôt, se laisser installer un boîtier connecté dans leur auto. Le but : leur fournir des informations, des services, et les alerter de la prochaine révision.**

En associant son application mobile, lancée en 2013, au boîtier connecté Xee, Norauto se dit désormais prêt à proposer un service d'un nouveau genre : la « révision connectée ». Alors que l'appli se limitait jusqu'alors au suivi des entretiens auto, elle sera bientôt capable de signaler aux automobilistes lorsqu'il est temps d'aller à la révision. Pour cela, l'enseigne équipera les voitures d'un petit appareil sur la prise diagnostic (OBD).
Fabriqué par la société lilloise Eliocity depuis l'automne 2014, Xee – concurrent des solutions Automatic ou Drust – a plusieurs fonctionnalités : localiser l'auto grâce à sa puce GPS, envoyer un SOS en cas de problème, déclencher une alerte s'il y a une effraction, aider à améliorer la conduite en observant le comportement du conducteur, et en lui prodiguant des conseils sur l'application (changements de rapports…), et d'autres.
Grâce à la connaissance du kilométrage en temps réel, l'application préviendra des révisions à venir, comme c'est déjà le cas dans certains véhicules haut de gamme. L'avantage pour le client est qu'aucune modification du véhicule n'est nécessaire pour le rendre compatible. La « révision connectée » sera dans un premier temps testée auprès d'un panel d'utilisateurs, afin de la peaufiner. Elle sera aussi limitée aux possesseurs d'iPhone.

**L'ambition de Norauto, grâce à Xee, est de personnaliser sa relation client**
À terme, l'application sera étendue à tous les automobilistes possédant un véhicule produit après 2000 – le plus susceptible d'embarquer une prise OBD – ainsi qu'à l'écosystème Android. Dans la mesure où Eliocity propose une plateforme ouverte aux développeurs, il est probable que de nouveaux services viennent enrichir l'application. Car la révision connectée n'est qu'une première étape. Plus tard, Norauto voudrait remonter davantage d'information de chaque véhicule, afin de personnaliser sa relation. Et attirer dans ses centres.

---



---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://pro.clubic.com/actualite-e-business/actualite-774146-norauto-inaugure-revision-connectee-boitier-xee.html
Par Thomas Pontiroli

---

# A Guédiawaye (Sénégal), la police démantèle un réseau de ressortissants nigérians | Le

# Net Expert Informatique

## A Guédiawaye (Sénégal), la police démantèle un réseau de ressortissants nigérians

**6 ressortissants nigérians ont été interpellés par les éléments de la Brigade de recherches du Commissariat de police de Golf Sud (Guédiawaye). Le matériel qui a été découvert chez eux a permis de conclure que ces derniers s'activaient dans la cybercriminalité, selon le journal Grand Place.**

La police de Guédiawaye (Sénégal) vient de démanteler un vaste réseau de cybercriminalité entretenu par des ressortissants nigérians. C'est suite à une information anonyme relative aux agissements répréhensibles de ces derniers que l'agent de police en chef de la commune de Golf Sud a mis sur pied un plan de neutralisation. Ainsi, ses hommes en civil se sont rendus sur les lieux dans la nuit du vendredis 10 juillet, aux environs de 23h, et ont pu arrêter 6 ressortissants nigérians.
Une perquisition de l'immeuble où ils ont été trouvés a permis de mettre la main sur 6 ordinateurs portables de marques différentes. L'exploitation des différents logiciels et autres systèmes des machines a permis la découverte d'installations et de fichiers de comptes bancaires de tiers ainsi que de faux documents étatiques et de réfugiés politiques.
Il y avait aussi plusieurs systèmes sur les ordinateurs portables avec des noms de code permettant à leurs propriétaires d'exercer, en toute discrétion, une activité criminelle.
– L'un permet d'effacer toutes les données après chaque redémarrage de l'outil informatique,
– alors que le deuxième est un système de navigation qui consiste à utiliser Internet sans pour autant être tracé ou repéré par les opérateurs de téléphonie.
– Et le troisième logiciel installé sur la machine ouvre la possibilité aux présumés cybercriminels de pirater les comptes bancaires d'autrui sans laisser des traces.

---



---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.leral.net/Cybercriminalite-a-Guediawaye-La-police-demantele-un-reseau-de-ressortissants-nigerians_a149877.html

# Le site de rencontre Madison Ashley piraté – l’analyse de Kaspersky Lab | Le Net Expert Informatique

| | |
|---|---|
|  | Le site de rencontre Madison Ashley piraté – l’analyse de Kaspersky Lab |

**Le site de rencontres adultères canadien Ashley Madison, qui revendique plus de 37 millions d'inscrits, a été victime d'une attaque informatique ayant pour but de voler les données personnelles d'un grand nombre d'utilisateurs. Ces données ont été brièvement mises en ligne.**

Marta Janus, chercheuse en sécurité au sein de l'équipe de recherche et d'analyse (GReAT) du spécialiste en sécurité Kaspersky Lab, revient sur cette attaque :
Marta Janus « L'attaque subie par Madison Ashley nous rappelle à quel point il est important pour toutes les entreprises de mettre en place des mesures de sécurité contre les cyberattaques, afin de protéger les données personnelles de leurs utilisateurs. Un internaute qui accepte de confier certaines de ses données privées à un site web devrait être assuré que ses informations seront conservées de la façon la plus sécurisée qui soit, et les entreprises concernées devraient pouvoir s'y engager.
Il faut également rappeler que toutes les failles de sécurité qui entrainent des fuites de données privées sont un problème, quelles que soit la nature du site visé, sa moralité et même sa légalité. Dans le cas de l'attaque contre Ashley Madison, l'affaire est très sérieuse car la fuite concerne des informations comme les noms, les adresses ou encore les données bancaires. Une fois rendues publiques, ces informations pourraient par exemple être utilisées pour voler de l'argent.
Les raisons pour lesquelles une entreprise peut être victime d'une cyber attaque sont nombreuses – argent, politique ou même éthique. N'importe quelle entreprise peut être la cible d'une attaque et même si les solutions de sécurité réduisent les risques que cette attaque soit fructueuse pour les criminels, d'autres mesures existent pour une protection renforcée. Je pense notamment aux mises à jour logicielles, encore trop souvent remises au lendemain, à la réalisation régulière d'audits de sécurité ou encore au test des infrastructures. Le meilleur moyen de lutter contre ce type de cyberattaques est de se protéger avant qu'elles ne frappent en disposant d'une stratégie de sécurité complète et efficace. »

---



---



---



Source : https://www.globalsecuritymag.fr/Site-de-rencontre-pirate-l-analyse,20150720,54540.html
par Kaspersky Lab

# Les entreprises attendraient-elles gentiment les attaques ? | Le Net Expert Informatique


## Les entreprises attendraient-elles gentiment les attaques ?

**Qu’on se le dise : n’importe qui peut se faire attaquer, qu’il s’agisse d’une petite comme d’une grande entreprise.**

En 2013, le New York Times a subit une cyberattaque de l’armée électronique syrienne ; un groupe d’activistes soutenant Bachard El Assad. Les auteurs ont ciblé la partie la moins sécurisée du réseau, les serveurs DNS alors qu’ils sont devenus la pierre angulaire de toute applications internes ou externes.
En juin dernier, l’US Army s’est faite attaquée par les mêmes hackers. Et ce, alors même que l’Etat--Major américain avait fait de la cyberdéfense une priorité en investissant fortement. Pourtant, ces deux attaques démontrent qu’ils sont faiblement protégés et que, quelque soit leur taille, toutes les entreprises ou organismes sont des cibles potentielles. Les services informatiques n’ont donc pas su s’adapter à ces nouvelles menaces.
En France, le 1er semestre fut dense en matière de cyberattaques : TV5 Monde, Charlie Hebdo et Thales ont fait l’objet de sévères attaques de leur système informatique. On se souvient que des documents présentés comme des pièces d’identité et des CV de proches des militaires français impliqués dans les opérations contre l’EI avaient été postés sur le compte Facebook de TV5Monde par les pirates.
L’attaque avait été initialement revendiquée par des inconnus se réclamant de Daech (Etat Islamique). L’enquête s’oriente en juin vers des hackeurs russes. Le vol de données semble être le principal objectif des hackers.
Quelques semaines plus tôt, Manuel Valls annonçait que la défense française allait intégrer des community managers et hackers, plus à même de contrer les attaques. Une méthode innovante…. mais est--ce suffisant pour protéger une infrastructure réseau ?

**Les entreprises françaises en mal d’inspiration ?**
En général, les entreprises ne communiquent pas ou très peu sur leurs attaques. En effet, en regardant de plus près les cyberattaques subies en France, on s’aperçoit que les informaticiens n’ont pas su anticiper les nouvelles menaces. Ils ont préféré sécuriser leurs réseaux grâce à des méthodes utilisées depuis des décennies. Malheureusement, cela ne s’avère plus suffisant pour contrer les nouvelles menaces et les nouvelles techniques utilisées par les hackers.
En parallèle, cela met en exergue les problèmes d’investissement que les entreprises rencontrent et leurs manques de réactions.
Selon une étude menée par IDC [1], si la plupart des organisations sont conscientes des risques de sécurité liés aux serveurs DNS (82 % des répondants étaient conscients des menaces, qu’ils ont reconnues), l’essentiel des budgets en sécurité réseau est encore consacré à des solutions de sécurité plus traditionnelles telles que les pare--feu (68 %).
L’étude d’IDC a également révélé que même si 85 % des répondants disposent des fonctions de sécurité du DNS de base, les entreprises restent vulnérables, car ces fonctions sont généralement inefficaces en cas d’attaque.
Enfin, 73% des entreprises françaises ont subies des attaques sur leurs serveurs DNS mais elles ne sont que 7% à les considérer comme une très grande menace contre 27% aux Etats-- Unis, alors que les dégâts subies lors de ces attaques ont été très importants (vol de données, interruption de service, …).
Sans prise de conscience des responsables informatiques français, les cyberattaques ne cesseront de s’intensifier. Avec la multiplication des appareils connectés à internet, dans tous les domaines d’activités (hôpitaux, grandes administrations ou petites entreprises, dans la banque, l’énergie, la défense,), les données continueront d’avoir de la valeur aux yeux des pirates informatiques si les RSI ne changent pas leurs méthodes de protection.

[1] Enquête IDC sur la sécurité des serveurs DNS, avril 2014

---



---



---



Source : https://www.globalsecuritymag.fr/Les-entreprises-attendraient-elles,20150715,54386.html
par Hervé Dhelin, Directeur Marketing d’EfficientIP